Desert Blue Connect is committed to protecting the privacy and confidentiality of clients. The Organisation will ensure that all personal and health information regarding clients and their families is collected, stored and used in accordance with statutory obligations (under the Privacy Act 1988) and best practice standards. Desert Blue Connect will promptly investigate, remedy and document any client grievance regarding privacy, dignity or confidentiality.

This policy outlines Desert Blue Connect employee's responsibilities in the management of personal, sensitive, confidential and private customer and employee information. It applies to all current and former Desert Blue Connect employees, as well as volunteers, work-experience people, students and stakeholders.

A copy of the Australian Privacy Principles may be obtained from the website of The Office of the Australian Information Commissioner at www.aoic.gov.au.

A copy of this policy is available on our website www.desertblueconnect.org.au. If a hard copy of this policy is requested by a client staff are to provide them with one.

Client files are the property of Desert Blue Connect and remain the property of the organisation, including after the cessation of client contact with the organisation. For information regarding minimum storage periods refer to Client Records Policy (COR-POL-001).

What is personal information and why do we collect it?

Personal Information is information or an opinion that identifies an individual. Examples of Personal Information we collect include: names, addresses, email addresses, phone and facsimile numbers.

This Personal Information is obtained in many ways including counselling, interviews, by correspondence, telephone, email and from third parties.

We collect Personal Information for the primary purpose of providing services and information to clients and marketing. Personal Information may also be used for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure. Clients may unsubscribe from our mailing/marketing lists at any time by contacting us in writing.

When we collect Personal Information we will, where appropriate and where possible, explain to the client why we are collecting the information and how we plan to use it.

Sensitive Information

Sensitive information is defined in the Privacy Act to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information.

Sensitive information will be used by us only:

- For the primary purpose for which it was obtained
- For a secondary purpose that is directly related to the primary purpose
- With your consent; or where required or authorised by law.

Third Parties

Where reasonable and practicable to do so, we will collect Personal Information only from the client. However, in some circumstances we may be provided with information by third parties. In such a case we will take reasonable steps to ensure that the client is made aware of the information provided to us by the third party.

Consent forms must be completed and signed prior to information being collected from other organisations. Clients must be informed as to what information is required and why it is required by Desert Blue Connect. This must be clearly documented.

Consent

Before collecting and/or releasing personal information, clients must be advised of the following:

- the purposes for which the information is collected;
- the right of the individual to view their personal information (except in certain circumstances) (refer to the Client Records Policy COR-POL-001);
- how information is stored;
- who has access to the information;
- the length of time information needs to be archived;
- how information is disposed of;
- associations to which Desert Blue Connect may disclose information, under what circumstances, and why such disclosure needs to occur;
- where the client is under the age of sixteen and not designated as mature minor, the fact that the custodial parent or guardian may be able to gain access to any information the association has about them.

Collection of Client Information:

Desert Blue Connect will take such steps (if any) as are reasonable in the circumstances to ensure that personal information collected is accurate, up-to-date, complete and not misleading as per Australian Privacy Principle 10.1 and 13.

For information on client record retention and disposal, refer to the Client Records Policy (COR-POL-001).

Photographic, video and digital images

Photographic, video or other identifying images of clients are not displayed or aired publicly without prior written permission of the client and/or parent guardian.

Prior consent must be obtained before counselling sessions are recorded for clinical Quality Assurance. All such recordings must be destroyed at the end of the Quality Assurance process and will not be used for any other purpose.

Support letters / Attendance summary

Support letters for clients may be written and supplied to the client by the staff involved in the case for advocacy purposes only, examples include letters for Department of Communities, Housing or childcare. These types of letters do not need approval from the CEO. This doesn't include any letters requested for legal matters.

Queries in relation to letters of support requested are to be discussed with the CEO.

A client's attendance summary for government departments may be written by staff with the clients consent.

Requests for documents for legal purposes

Requests from clients / lawyers / other departments for Desert Blue Connect to provide:

- a letter of support for court or other legal purposes
- a report regarding the client
- support letter or documents in regard to immigration status
- Any written information requested from clients is to be kept to the minimum necessary to provide adequate and appropriate service to them.
- All such requests must be in writing and addressed to the CEO. All such requests must include a reason for the production of the requested document and be specific in type of information they require.
- Desert Blue Connect may refuse production of such a document and in such cases will provide feedback to the person requesting. All such documents must have approval of the CEO prior to being provided to the client.

There is a fee associated with accessing documentation, payable by EFT, Cheque or Money Order, prior to work being undertaken. Refer to Fee Schedule (COR-FRM-013)

Clinical Practice, Accountability and Reporting Provisions

The CEO has full access to all clinical notes and other documentation for the purposes of quality assurance, and to make informed decisions when required, but will only access notes on a need-to-know basis.

The CEO may also from time to time view or organise to have recorded clinical sessions for the purposes of quality assurance. Prior consent from clients must be obtained for these purposes, and all such recordings will be destroyed at the end of the QA process, and will only be used for the purposes specified in the consent.

Counsellors may discuss scenarios using non-identifying client details at external supervision sessions.

The Administration staff may be privy to some statistical information for data entry purposes and funding agency statistics. Refer to the Client Records Policy (COR-POL-001).

Reporting

Only *non-identifying* client statistics may be utilised for reporting purposes. Any information used outside reporting purposes such as research is to be presented to the Board for ethical and best practice consideration.

Disclosure of Personal Information

Personal Information may be disclosed in a number of circumstances including the following:

- Third parties where the client consents to the use or disclosure. Written consent must obtained from the client and/or their parent/guardian prior to releasing information to any other sources except where the organisation is required by law to disclose the information, using the Consent to Share Information Form (SD-FRM-005). This includes any acknowledgement that the client is known to Desert Blue Connect.
- Where required or authorised by law.

Exceptions to Confidentiality

No information must be disclosed to any parties except under compulsion of law, with consent or due to overwhelming public interest (to be determined by CEO in consultation with the Desert Blue Connect Board). Where such disclosure is deemed necessary, only relevant, accurate, up-to-date and complete personal information must be provided as, required by Australian Privacy Principle 10.

- *Compulsion of Law*
    - Confidential information is not privileged from disclosure to a Court, either as a witness or in answer to a subpoena to produce documents. However, all requests for information from police, coroner's inquiries and other legal bodies should be denied until the appropriate Court Orders (subpoena, search warrant, etc.) are produced.

    - Any requests for information under a Court Order should be immediately referred to the CEO and such orders must be considered in conjunction with the Subpoenas and Search Warrants Policy (COR-POL-016).

- Mandatory reporting by doctors and nurses who must comply with Children and Community Services Act (2004) to report child sexual abuse.

- *Circumstances where a Counsellor becomes privy to ongoing physical, emotional, sexual maltreatment or neglect of a mature minor (aged 14-18years)*.
  - When appropriate, the Counsellor should discuss the matter with the client first, then the CEO. The CEO will make the decision: whether the authorities (and which ones) are to be notified, especially if a family member is involved; when the client will be notified that report has be made to relevant authorities and when this occurred. Refer to the Child Protection Policy (COR-POL-007).

- *Consent*
  - Custodial parents/guardians can consent to disclosure for clients who are under sixteen years of age. In these cases, written consent must be obtained before the information is disclosed using the appropriate consent forms. The parent/guardian *may* have a right to information regarding the child's general progress and any serious concerns for the child's psychological, emotional or physical well-being, depending on the nature of their current relationship with the child. All such cases must be discussed with the CEO prior to the release of any information.

- *Overwhelming Public Interest*
  - Disclosure is allowed in circumstances where there is actual or threatened risk to life or health (for example advising the Health Department of a notifiable disease), or where there is advance knowledge of the intent to commit a serious crime.

  - This relates to people in danger of imminent self-harm or of harming others, or people who disclose their intention to commit a serious crime. Disclosure should be to the appropriate authorities (e.g. the Department of Child Protection and Family Support or Acute Care Hospitals) and be limited to the nature of the risk and to who is at risk.

  - Event assessed by Counsellor to be life threatening to a client or others (with the event of phone call): Return telephone contact will be immediately made with the client to assess circumstance, need for follow-up counsel or provision of referral to a crisis agency. At no time is a Desert Blue Connect staff member to directly intervene outside of Desert Blue Connect's premises or business hours. Where the event is on Desert Blue Connect premises, refer to the Responding to Critical and Serious Incidents Policy (COR-POL-013).

The CEO must be notified prior to any disclosure unless it is a life threatening emergency and the delay would cause further harm, in which case the CEO is be notified following the situation.

Data Breaches

All client information is considered data. Access to date (client information) is strictly limited to Desert Blue Connect employees and the Desert Blue Connect Board where access is necessary for the provision of services and/or risk management. All employees are responsible for ensuring clients privacy and confidentiality. This includes ensuring that no unauthorised access, unauthorised disclosure or loss of client information occurs. If an employee identifies a breach has occurred (or suspects) they must report it immediately to the CEO/OM so remedial action can be taken. Failure to report a breach (or suspected breach) may result in disciplinary action up to and including dismissal.

Any previous Desert Blue Connect employee found to be in breach of client confidentiality and therefore the Code of Conduct may be subject to legal action, dependent upon the circumstances and severity of the breach.

Data breaches include:

Unauthorised access of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

Unauthorised disclosure occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity, and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.

Loss refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure. An example is where an employee of an entity leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport.

For management of data breaches refer to Data Breach and Response Plan COR-POL-023.

Practices to ensure privacy and confidentiality.

Interviews/counselling sessions will be conducted in a room where privacy can be assured. Door closed.

Staff will be careful to ensure that they avoid both intentional and all behaviours that could lead to unintentional breaches. These situations may include:

- speaking with others (including speaking with clients too loudly)
- speaking too loudly on the phone or giving clients results over the phone in hearing of others.

- reading referral letters or GP' s notes
- leaving personal records on the desk (hard copy and electronic)
- Discussing client information in the workplace other than on a "must know" basis; that is person being provided with information must have to know the information in order to provide a service to the client.
- Leaving information (appointment schedules etc.) visible on the computer screens.
- Discussing information with other staff who do not meet the "must know" requirement, or in hearing of others.
- Discussing results with relatives without the client's permission (especially the elderly and mature minors).

Staff will adhere to the following practices to prevent breaches:

- After hours hard copy client information must be stored securely in a locked cabinet, keys only available to authorised staff. During office hours documents must be kept out of reach of other clients, face down, with names not visible.
- Client information stored in a secure electronic database must be password protected. When leaving their desk staff are required to log off electronic databases.
- All staff have been allocated an individual log on and password for computer access. Staff must not share or disclose their password with anyone else and must not save their password on the computer.
- Staff are to ensure they return their computer to a neutral screen when they leave their desk. Screen savers have been installed on all computers and when activated staff are required to enter their password to access the computer again.
- Utilise background music in waiting rooms/hallways.
- Not removing or copying client or personnel files (or individual sections) from the premises unless you have been given permission to do so by the CEO/OM
- No personal information about clients, including their names, is kept on whiteboards, noticeboards or other locations where members of the public may view it.

RELATED DOCUMENTS

Client Records	COR-POL-001
Subpoenas & search warrants	COR-POL-016
Child Protection	COR-POL-007
Responding to Critical and Serious Incidents	COR-POL-013
Consent to Share Information	COR-FRM-005
Responding to reports of child abuse	COR-FRM-001
Media Permissions	COR-FRM-020
Data Breach and Response Plan	COR-POL-023
Student	

EXTERNAL DOCUMENTS

Privacy Act 1988
Australian Privacy Principles (APP)
Children and Community Services Act (2004)